#2

op1185

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　６月１６日

出願番号
Application Number: 特願２０００－１８２０１５

出願人
Applicant(s): 株式会社　イオノス

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　５月１１日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０４０１７８

【書類名】　特許願
【整理番号】　P-7600
【提出日】　平成12年 6月16日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 13/00
【発明の名称】　通信路のスイッチ接続制御装置
【請求項の数】　5
【発明者】
【住所又は居所】　東京都世田谷区宮坂１丁目３６番１８号　株式会社　イオノス内
【氏名】　星野　博一
【特許出願人】
【住所又は居所】　東京都世田谷区宮坂１丁目３６番１８号
【氏名又は名称】　株式会社　イオノス
【代理人】
【識別番号】　100089244
【弁理士】
【氏名又は名称】　遠山　勉
【選任した代理人】
【識別番号】　100090516
【弁理士】
【氏名又は名称】　松倉　秀実
【連絡先】　０３－３６６９－６５７１
【手数料の表示】
【予納台帳番号】　012092
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1

【物件名】　　要約書　1

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　通信路のスイッチ接続制御装置

【特許請求の範囲】

【請求項１】　通信路に介在され、一方側の通信路との接続と、他方の通信路との接続とを排他的に選択する通信路のスイッチ接続制御装置。

【請求項２】　データの検証および制御を行う主制御装置と、

第１の通信路と接続された第１のバッファと、

前記主制御装置に接続され要求またはデータを蓄積する第２のバッファと、

前記第１のバッファと第２のバッファとを短絡・開放する第１のスイッチと、

前記主制御装置と第２の通信路とを短絡・開放する第２のスイッチと、

前記主制御装置からの指示により、前記第１または第２のいずれか一方のスイッチを排他的に短絡させるための制御信号を出力するスイッチ管制部とからなる通信路のスイッチ接続制御装置。

【請求項３】　前記第１のバッファは、第１の通信路からの要求またはデータの正当性を検証する検証手段を備えた請求項１記載の通信路のスイッチ接続制御装置。

【請求項４】　前記主制御装置は、第２の通信路からの要求またはデータの正当性を検証する検証手段を備えた請求項１記載の通信路のスイッチ接続制御装置。

【請求項５】　前記に加えて、主制御装置と第２のスイッチとの間に要求またはデータを蓄積する第３のバッファと、

前記第２の通信路と前記第２のスイッチとの間に要求またはデータを蓄積する第４のバッファとを備えた請求項２記載のスイッチ接続制御装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークにおけるセキュリティに適用して有効な技術に関する

。

【０００２】

【従来の技術】

インターネットの普及は、ビジネス形態を根本から変えるといわれている。

【０００３】

データセンターやプロバイダー事業はおろかエンドユーザーまでが、インターネットに常時接続されている昨今、不正なアクセスによる犯罪が盛んになりつつある。いまやセキュリティの導入は政府機構から一個人までその必要性に迫られている。

【０００４】

外部ネットワーク（インターネット等）から内部ネットワーク（イントラネット）へのアクセスを防止するためにファイアウォール技術が知られている。

【０００５】

このような従来技術のセキュリティは、すべての端末及びシステムが物理上あるいは論理上一本のラインでつながっており、ファイアウォールにより論理的に適正を判断していた。

【０００６】

【発明が解決しようとする課題】

従来のネットワークセキュリティ技術では、すべての端末及びシステムが物理上あるいは論理上一本のラインでつながっているため、不正な侵入が可能であるという問題点を抱えている。

【０００７】

このためには、外部ネットワークと内部ネットワークとを切り離すことが最も安全である。すなわち、どのような事態（破壊攻撃等）においても一本のラインでつながることがないため、不正な侵入を防御できる。

【０００８】

ところが、外部ネットワークから内部ネットワークに対してのアクセス、あるいは内部ネットワークから外部ネットワークへのアクセスが完全に遮断されてしまうと、ネットワーク相互の柔軟な運用が不可能となってしまう。

【０００９】

つまり、外部ネットワークと内部ネットワークとを物理的に切り離すことはリ

アルタイム性や双方向性が損なわれる恐れがある。

【００１０】

本発明は、外部ネットワークからのアクセスに対し、物理的手段によって内部ネットワーク内への直接的な侵入を防ぎつつ、内部ネットワークと外部ネットワークとの柔軟な連携を可能とすることを技術的課題とする。

【００１１】

【課題を解決するための手段】

本発明は、通信路に介在され、一方側の通信路との接続と、他方の通信路との接続とを排他的に選択する通信路のスイッチ接続制御装置である。

【００１２】

すなわち、目的別に分散した端末及びシステムに、シーソー式のスイッチング技術を用い不正侵入を防ぐセキュリティシステムを提供する。

【００１３】

シーソー式のスイッチング技術により、物理的に外部ネットワークと内部ネットワークとを目的に応じたアクセス要求の制御信号によって切り離すため、不正行為から確実にデータを守ることが可能となる。

【００１４】

【発明の実施の形態】

【００１５】

【実施例】

以下、図面に基づいて、本発明の実施の形態を説明する。

【００１６】

図１は、本発明の概念を示す機能ブロック図である。

【００１７】

図1に示すように、目的別の端末及びシステムを以下の３つに分類・分散する。

【００１８】

同図中、１は、重要なデータやシステムを保有する内部ネットワークであり、コンピュータシステムを通信回線で接続した汎用のネットワークで構成されてい

る。ここで、内部ネットワークとは、上記に示す有線あるいは無線を含めた外線と繋がっていない端末あるいはネットワークを有するシステムを内部ネットワークという。

図中２は外部ネットワークである。ここで外部ネットワークとは、インターネット網あるいは公衆網あるいは専用線等の有線あるいは無線を含めた外線と繋がっているネットワークあるいはネットワークを有するシステムあるいは端末あるいはモジュラージャック等のネットワーク構成部品を外部ネットワークという。

３は、本発明の最も重要な要素となる、内部ネットワークと外部ネットワークとを制御するための制御端末（シーソー式スイッチングセキュリティシステム）である。

【００１９】

制御端末３は、さらに、スイッチサーバ３１、スイッチ管制部３２、バッファ３３、バッファ３４およびシーソースイッチングボックス（ＳＳＷＢ）３５とで構成されている。これらの各機能部については後で詳述する。

【００２０】

このシステムにおいて、制御端末３は、図２に示すように、外部ネットワークからの要求を受信し、内部ネットワークへ送信する機能を有している。また、内部ネットワークのデータを受信し、外部ネットワークへ送信する機能を有している。同図において、シーソースイッチングボックス（ＳＳＷＢ）５は、外部ネットワーク２からの要求信号を内部ネットワーク１に伝えるために、バッファ３４をバッファ３３と接続した状態となっている。

【００２１】

また、制御端末３は、図３に示すように、内部ネットワークからの要求を受信し、外部ネットワークへ送信する機能を有している。また、外部ネットワークのデータを受信し、内部ネットワークへ送信する機能を有している。同図において、シーソースイッチングボックス（ＳＳＷＢ）５は、内部ネットワーク１からの要求信号を外部ネットワーク２に伝えるために、内部ネットワーク１とスイッチサーバ３１とを接続した状態となっている。

【００２２】

制御端末３はまた、図４に示すように、内部ネットワーク１または外部ネットワーク２の双方において、要求信号、データ信号を双方向に送受信することも可能である。

【００２３】

このような双方向のモードで使用する場合には、スイッチサーバ３１とシーソースイッチングボックス（ＳＳＷＢ）３５との間にバッファ３７を介装し、さらに内部ネットワーク１とシーソースイッチングボックス（ＳＳＷＢ）３５との間にもバッファ３６を介装して、制御端末３内が内部ネットワーク１、外部ネットワーク２に対して左右対称構成となるようにしてもよい。この場合、バッファ３６は、内部ネットワークからの要求を外部側スイッチ（ＳＷ２）が閉じるまで、保持する。また、内部ネットワークからの要求に不正なデータがないかを判断し、不正データが検出されるとその要求を破棄するフィルタリングの機能を有する。

【００２４】

バッファ３７は、外部ネットワーク２からのデータをスイッチサーバ３１が受け、適正処理されたデータを内部側スイッチ（ＳＷ２）が閉じるまで、保持する機能を有している。

【００２５】

その他の制御端末３の動作については、前述の図２乃至３で説明したものと同様であるので説明は省略する。

【００２６】

なお、制御端末３内を左右対称構造としたものは図４だけで示したが、このような構造は制御端末３をいずれのモードで使用した場合にも適用可能である。

【００２７】

次に、図５を用いて、本実施例のオブジェクト分散型ユニット（目的別によって分散されたユニット）における各ユニットの構成、機能及びその動作を説明する。

【００２８】

スイッチサーバ３１は、コンピュータシステムにより構成されており、バスを

中心に中央処理装置（ＣＰＵ）、メモリ、外部記憶装置、インターフェース（Ｉ／Ｏ）等で構成されている。外部記憶装置にはプログラムがインストールされており、中央処理装置（ＣＰＵ）は当該プログラムをメモリにロードして順次実行することによって、スイッチ管制部３２に対してシーソースイッチングボックス（ＳＳＷＢ）３５の制御指示信号を出力するようになっている。

【００２９】

つまり、スイッチサーバ３１は、外部ネットワークからの要求により、内部ネットワークへ必要なデータを要求したり、内部ネットワークから受け取ったデータと外部ネットワークからの要求の整合性を図る等、目的に応じた処理を行う。また、要求やデータ等の信号を元に外部ネットワーク側と内部ネットワーク側のそれぞれのゲート（ＳＷ１及びＳＷ２）を排他的に切り替える為の制御信号をスイッチ管制部３２に送る。

【００３０】

スイッチ管制部３２は、中央処理装置（ＣＰＵ）およびメモリを中心に複数のインターフェース（Ｉ／Ｏ）で構成されている。すなわち、スイッチサーバ３１からの制御指示信号に基づいてシーソースイッチングボックス（ＳＳＷＢ）３５を制御するようになっている。

【００３１】

ここで、スイッチ管制部３２は、ネットワーク上のデータ信号経路にまったく接触しておらず、スイッチサーバ３１、バッファ３４、バッファ３３、シーソースイッチングボックス（ＳＳＷＢ）をそれぞれ監視することで、ユニットの状態を管理する役割を有している。

【００３２】

そして、バッファ３４、バッファ３３に対しては、スイッチサーバ３１等からの情報を元に各々のモード変更の制御信号を送る。（図１３乃至１４を参照）

また、スイッチサーバ３１に対しては、上記のバッファ３４，３３のモード状態信号を送る。また、スイッチサーバ３１からシーソースイッチングボックス（ＳＳＷＢ）３５へのスイッチ切り替え制御信号を受け、バッファ３４，３３のモード状態との適正を判断し、シーソースイッチングボックス（ＳＳＷＢ）に対し

てスイッチ切り替え制御信号を送る機能を有している。

【００３３】

バッファ３３および３４はほぼ同様の構成を有しているが、バッファ３４は外部ネットワークに直接接続されている点、バッファ３３はシーソースイッチングボックス（ＳＳＷＢ）３５とスイッチサーバ３１との間に介装されている点が異なる。

【００３４】

バッファ３４は、外部ネットワークからの要求を外部側スイッチ（ＳＷ２）が閉じるまで、保持する。また、外部ネットワークからの要求に不正なデータがないかを判断し、不正データが検出されるとその要求を破棄するフィルタリングの機能を有する。

【００３５】

バッファ３３は、内部ネットワークからのデータをスイッチサーバ３１が受け、適正処理されたデータを外部側スイッチ（ＳＷ２）が閉じるまで、保持する機能を有している。

【００３６】

シーソースイッチングボックス（ＳＳＷＢ）３５は、フリップフロップ素子（ＦＦ）と、スイッチ（ＳＷ１，ＳＷ２）とで構成されており、フリップフロップ素子（ＦＦ）に入力されるスイッチ管制部３２からの指示信号Ｔの値によって、スイッチ１または２のいずれかのスイッチを短絡状態に制御するようになっている。

【００３７】

つまり、シーソースイッチングボックス（ＳＳＷＢ）３５は、スイッチ管制部３２からの制御信号を受け、フリップフロップ（ＦＦ）の動作により、外部ネットワーク２側と内部ネットワーク１側のスイッチ（ＳＷ１及びＳＷ２）を排他的に切り替える機能を有している。この点については、図６に真理値表を示してシーソースイッチングボックス（ＳＳＷＢ）の動作アルゴリズムを説明している。

【００３８】

このように、本実施例では、上記に示す各ユニットが、各々明確な役割を持ち

、独立・分散していることで、クラッキング行為や不正侵入から大切なデータを守ることができる。特に、スイッチ管制部３２がネットワーク上のデータ信号経路にまったく接触していないため、スイッチサーバ３１やバッファ３３，３４がクラックされたとしても、それを察知し、シーソースイッチングボックス（ＳＳＷＢ）を制御することができる。

【００３９】

この制御方法を利用して、スイッチサーバ３１やバッファ３３，３４をデュープレックス構造にすれば、クラッキングされたユニットを予備のユニットに自動的に切り替える強化型セキュリティシステムを構築できる。

【００４０】

なお、実際の運用に際してスイッチサーバ３１が運用モード切替指示（図１５のタイミングチャート）を出力するタイミングとしては、以下のようなパターンが考えられる。

【００４１】

（１）スイッチサーバへの要求が少ない時間帯に切り替える。

【００４２】

スイッチサーバ３１へのアクセス状況を基に要求の少ない時間帯を調べ、その時間帯にスイッチサーバへ外部の要求を受け付けられないと、ユーザーには知らせ、その間に内部ネットワークとの通信を行う。

（２）定期的に切り替える。

【００４３】

要求のとぎれる時間帯がない場合、あらかじめ指定した時間ごとに接続を外部から内部へ切り替える。切り替える回数を増やすことで１回あたりの内部との通信にかかる時間を減らして、ユーザーの外部ネットワークから要求の遅延を減らすことができる。

（３）ユーザーの要求ごとに切り替える。

【００４４】

例えば、内部ネットワークに蓄積している個人情報のうち、ある特定個人の情報を見たい、というアプリケーションの時に、個人情報の問い合わせの都度接続を切り替える。必要最低限の情報のみを外部ネットワーク側へ流すことで、情報を守ることができる。

以上のような（１）乃至（３）の制御は、スイッチサーバ１の記憶装置にインストールされたプログラムに基づいて行われる。

【００４５】

次に、図７乃至図１０を用いて、本システムの動作を説明する。

【００４６】

本システム（ＳＷＳＥＣ）内は、物理的に外部ネットワーク２側のスイッチ（ＳＷ２）または内部ネットワーク１側のスイッチ（ＳＷ１）のいずれか一方しか閉じない（短絡しない構造の）ため、たとえＳＷＳＥＣシステムのスイッチングを制御するスイッチ制御指令または情報受発信サーバ（ここではスイッチサーバ３１）がクラッキングされても、内部ネットワークと外部ネットワークが電気的に導通することはない。

【００４７】

また、ネットワーク上のデータ信号経路にまったく接触していない各ユニット（スイッチサーバ３１、バッファ３４、バッファ３３の）制御及び監視機構（ここではスイッチ管制部３２）を配置し、スイッチ制御を行うことでクラッキングによる外部からの制御を受付けないようにしている。

【００４８】

ここでは、スイッチ３５を制御するタイミングを、ＳＷＳＥＣシステムが自律的にスイッチングする訳ではなく、スイッチサーバ３１が制御指令を出すことにより、外部ネットワーク２から要求の無いときにもスイッチングを行うことができる。スイッチングによって、外部ネットワーク２と切断されている間に要求があった場合は、バッファ３４に当該要求が蓄積され、ＳＷＳＥＣシステムの接続が外部ネットワーク２側に切り替わった際に当該要求がバッファ３４からスイッチサーバ３１に伝送される。

【００４９】

スイッチサーバ３１と外部ネットワーク２の伝送が途切れなく続く場合は、定期的に内部ネットワーク１に接続する時間を設け、守るべきデータを内部ネットワーク１に伝送する。伝送中にスイッチサーバ３１から発信すべきデータは、バッファ３３に蓄積される。また、伝送量が多い場合は、守るべき情報以外がはいっている情報サーバ（図示せず）を外部ネットワーク側に設けることで、守らなくてよい情報に対するリクエストを常時受け付けることができる。

【００５０】

次に動作を説明する。

【００５１】

外部ネットワーク２側から内部ネットワーク１に対して要求があるとその要求信号は、バッファ３４に蓄積される。

【００５２】

ここで、要求が不正なものか正当なものかをバッファ３４内の中央処理装置（ＣＰＵ）が外部記憶装置にインストールされたフィルタプログラムを用いて判断し、不正なものであればその要求を破棄する。

【００５３】

次に、シーソースイッチングボックス（ＳＳＷＢ）のスイッチ（ＳＷ２）が切断（開放）されている状態（内部ネットワーク１とスイッチサーバ３１とがデータ通信を行っている状態）を示すパケットバッファモードであれば、要求はバッファ３４に蓄積され、シーソースイッチングボックス（ＳＳＷＢ）のスイッチ（ＳＷ２）が接続される状態（内部ネットワーク１とスイッチサーバ３１がデータ通信を終了している状態）を示すパケットスルーモードになるまで待機する。

【００５４】

内部ネットワーク１とスイッチサーバ３１がデータ通信を終了するとスイッチサーバ３１がスイッチ管制部３２にシーソースイッチングボックス（ＳＳＷＢ）３５のスイッチの接続をスイッチ（ＳＷ１）からスイッチ（ＳＷ２）に切り替えるための制御信号を送出する。この制御信号を受け取ったスイッチ管制部３２は、バッファ３４及びバッファ３３の状態がパケットバッファモードになっている

かパケットスルーモードになっているかを監視し、パケットバッファモードになっていれば、パケットスルーモードにするための制御信号を各々バッファ３４、３３に送出する。そして、パケットバッファモードに変更した通知を示す制御信号を各々バッファ３４，３３から受け取ると、シーソースイッチングボックス（ＳＳＷＢ）に対してスイッチの接続をＳＷ１からＳＷ２に切り替えるための制御信号を送出する。また、パケットスルーモードになっていれば、シーソースイッチングボックス（ＳＳＷＢ）３５にスイッチの接続をＳＷ１からＳＷ２に切り替えるための制御信号を送出する。

【００５５】

前記要求は、シーソースイッチングボックス（ＳＳＷＢ）のスイッチ（ＳＷ２）及びバッファ３３を経由して、スイッチサーバ３１（スイッチング制御及び情報受発信サーバ）に入力される。

【００５６】

スイッチサーバ３１では、前記で入力された要求の適正及び目的を、中央処理装置（ＣＰＵ）がフィルタプログラムを用いて判断し、不正なものであればその要求を破棄する。

【００５７】

要求が適正である場合には、シーソースイッチングボックス（ＳＳＷＢ）３５のスイッチの接続をＳＷ２からＳＷ１に切り替えるための制御信号をスイッチ管制部３２に送る。

【００５８】

この制御信号を受信したスイッチ管制部３２は、バッファ３４及びバッファ３３の状態をパケットバッファモードにするための制御信号を各々バッファ３４、３３に送出する。そして、パケットバッファモードに変更した通知を示す制御信号を各々バッファ３４，３３から受け取ると、シーソースイッチングボックス（ＳＳＷＢ）３５に対してスイッチの接続をＳＷ２からＳＷ１に切り替えるための制御信号を送出する。

【００５９】

次に、スイッチ管制部３２から送られてきた制御信号をシーソースイッチング

ボックス（ＳＳＷＢ）３５が受け取るとフリップフロップ（ＦＦ）の動作により、スイッチの接続をＳＷ２からＳＷ１に切り替える（図８参照）。

【００６０】

スイッチサーバ３１は、内部ネットワーク１側に目的に合った要求を送出する。

【００６１】

次に、内部ネットワーク１は、図９に示すように、スイッチサーバ３１より送られてきた要求により、データを送出する。

【００６２】

当該データは、シーソースイッチングボックス（ＳＳＷＢ）の短絡状態のスイッチ（ＳＷ１）を経由して、スイッチサーバ３１に送られる。

【００６３】

スイッチサーバ３１は、そのデータを目的に合った適正な形式に形成する。この成形は外部記憶装置にインストールされたプログラムに基づいて中央処理装置（ＣＰＵ）が行う。

【００６４】

次に、スイッチサーバ３１は、シーソースイッチングボックス（ＳＳＷＢ）のスイッチの接続をＳＷ１からＳＷ２に切り替えるための制御信号をスイッチ管制部３２に送ると同時に、パケットバッファモードになっているバッファ３３に前記で成形されたデータを送出する。

【００６５】

スイッチサーバ３１からの制御信号を受け取ったスイッチ管制部３２は、シーソースイッチングボックス（ＳＳＷＢ）３５にスイッチの接続をＳＷ１からＳＷ２に切り替えるための制御信号を送出する。続いて、バッファ３３の状態をパケットスルーモードにするための制御信号をバッファ３３に送出し、パケットスルーモードに変更した通知を示す制御信号をバッファ３３から受け取る。

【００６６】

次に、図１０に示すように、データがバッファ３３からシーソースイッチングボックス（ＳＳＷＢ）３５のスイッチ（ＳＷ２）を経由して、パケットバッファ

モードになっているバッファ３４に入力される。

【００６７】

バッファ３３は、データを送信し終わるとその通知信号（バッファエンプティ信号）をスイッチ管制部３２に送出する。バッファエンプティ信号を受け取ったスイッチ管制部３２は、パケットバッファモードになっているバッファ３４に対してパケットスルーモードにするための制御信号を送出する。

【００６８】

この制御信号を受け取ったバッファ３４は、自身の状態をパケットスルーモードにし、パケットスルーモードに変更した通知を示す制御信号をスイッチ管制部３２に返信する。

【００６９】

このようにしてデータが外部ネットワーク２に伝送される。

次に、本実施例の適用例を図１１を用いて説明する。

【００７０】

同図では、たとえば、インターネットショッピングにおける個人ＩＤとユーザー属性の認証行為をプロバイダに置いているウェブサーバ１１０２から企業内に設置されたデータサーバ（内部ネットワーク１）へ要求された場合を想定している。

【００７１】

外部ネットワーク２は、インターネット２１に接続されており、当該インターネット２１は、ルータ１１０１を介してプロバイダのウェブサーバ１１０２に接続されている。このウェブサーバ１１０２は、ルータ１１０３を介してインターネット２２に接続され、当該インターネット２２にはユーザ端末１１０４が接続されている。

【００７２】

同図の場合、外部ネットワーク２からの認証要求に基づいて内部ネットワーク１から認証結果をデータとして出力する動作を行うが、この動作は前述の図７乃至図１０の説明で実現される。

【００７３】

図１２は、個人の家庭内に設置された端末装置２１が内部ネットワークに該当し、外部ネットワークであるプロバイダのウェブサーバ１２０３に対して楽曲データのダウンロード要求を送信し、これに対してウェブサーバ１２０３から楽曲データを受信する場合の構成である。

【００７４】

同図において、ルータやモジュラージャック２１を介して、インターネット１２０１に接続されており、当該インターネット１２０１は、ルータ１２０２を経由してプロバイダのウェブサーバ１２０３に接続されている。ウェブサーバ１２０３には音楽配信用の楽曲データが蓄積されている。

【００７５】

このような音楽配信サービスにおいて、個人の端末装置１１からウェブサーバ１２０３に対して楽曲データの送信を要求する。当該要求がウェブサーバ１２０３で受信されこれが図示しない方法で認証されると、ウェブサーバ１２０３から楽曲データがインターネット１２０１を介してルータ及びモジュラージャック２１を経由して制御端末３に受信される。このときの要求の発信からデータの受信の手順については、前述の図７乃至図１０の説明で同様に実現することができる。ただし、前述の図７乃至図１０の説明において、「要求」を「データ」、「データ」を「要求」と読み替える必要がある。

【００７６】

また、以上の適用例以外にも、企業内ＬＡＮやプロバイダー内、データセンター事業、個人用ＰＣ端末などにおいても本システムを介在させることが可能である。すなわち、本発明は、前述の実施例およびその適用例に限定されるものではなく、ネットワーク上の如何なる部分にも介在させることができ、ネットワーク毎の内部セキュリティを維持することが可能である。

【００７７】

【発明の効果】

本発明によれば、外部ネットワークと内部ネットワークとを目的に応じたアクセス要求の制御信号によって切り離すため、リアルタイム性や双方向性が損なわ

れることなくデータのやり取りが可能となる。

【図面の簡単な説明】

【図１】　本発明の原理構成を示すブロック図（１）

【図２】　本発明の原理構成を示すブロック図（２）

【図３】　本発明の原理構成を示すブロック図（３）

【図４】　本発明の原理構成を示すブロック図（４）

【図５】　実施例の詳細な機能ブロック図

【図６】　実施例のシーソースイッチングボックス（ＳＳＷＢ）の構成および真理値表

【図７】　実施例の接続制御装置動作説明図（１）

【図８】　実施例の接続制御装置動作説明図（２）

【図９】　実施例の接続制御装置動作説明図（３）

【図１０】　実施例の接続制御装置動作説明図（４）

【図１１】　実施例の適用例を示すシステム図（１）

【図１２】　実施例の適用例を示すシステム図（２）

【図１３】　実施例において外部通信モードから内部通信モードへの移行手順を示すフロー図

【図１４】　実施例において内部通信モードから外部通信モードへの移行手順を示すフロー図

【図１５】　実施例の接続制御装置のタイミングチャート

【符号の説明】

１　内部ネットワーク

２　外部ネットワーク

２１　インターネット

２２　インターネット

３　制御端末（制御装置）

３１　スイッチサーバ

３２　スイッチ管制部

３３　バッファ（第２バッファ）

３４　バッファ（第１バッファ）

３５　シーソースイッチングボックス（ＳＳＷＢ）

１１０１　ルータ

１１２０　ウェブサーバ

１１０３　ルータ

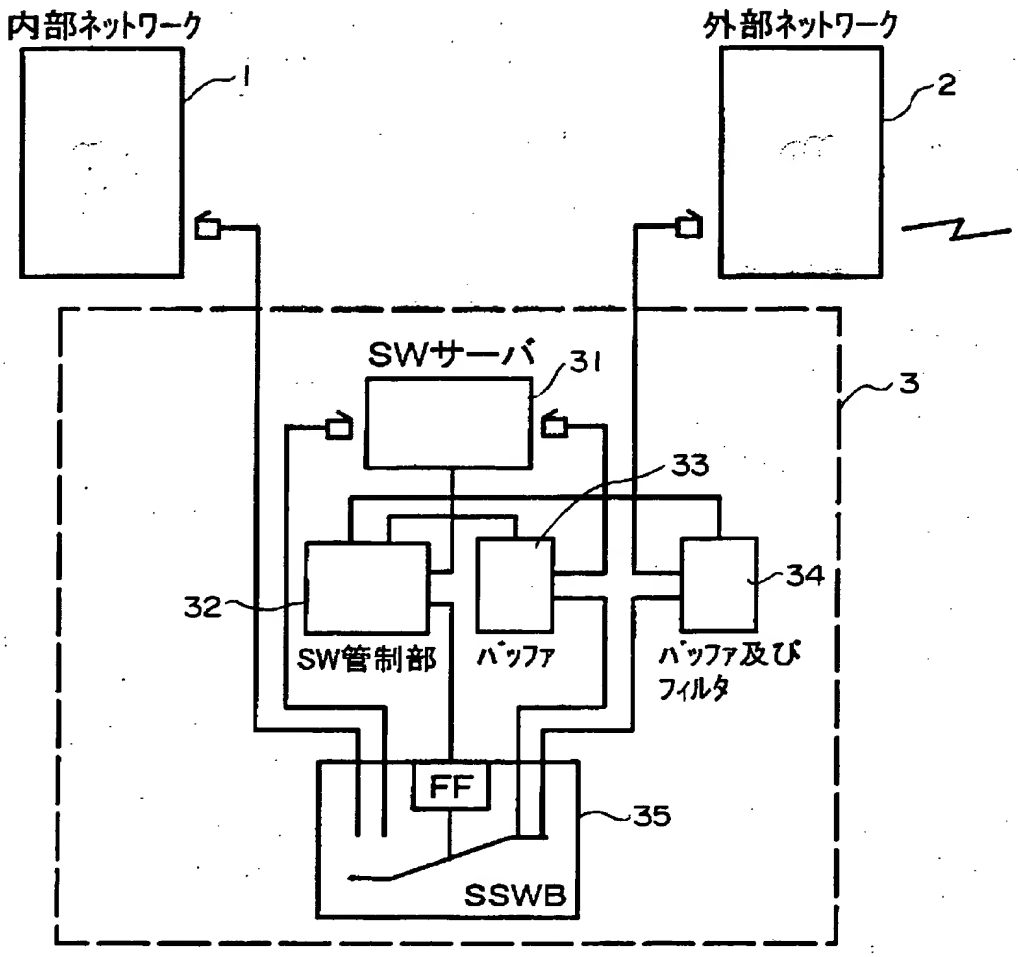
１１０４　ユーザ端末

１２０１　インターネット

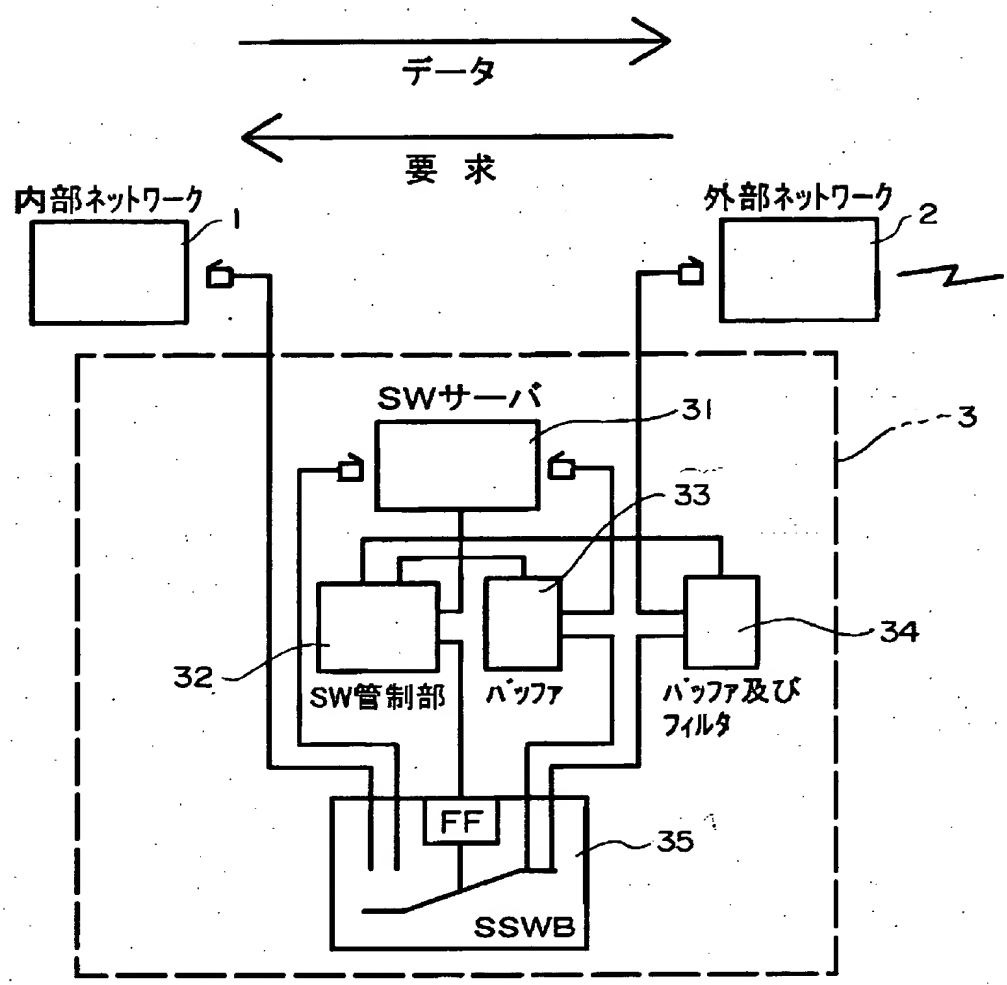
１２０３　ウェブサーバ

【書類名】　　図面

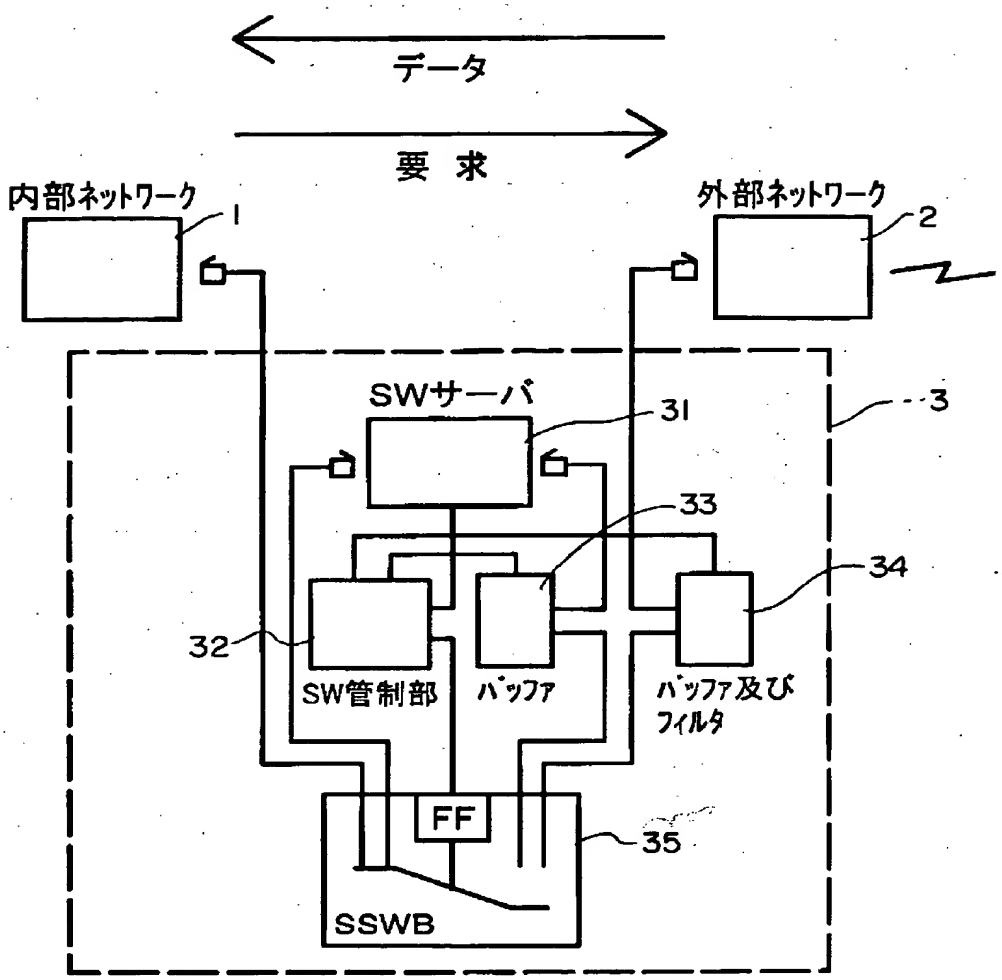
【図１】


内部ネットワーク
1
外部ネットワーク
2
SWサーバ
31
3
33
32
34
SW管制部
バッファ
バッファ及び
フィルタ
FF
35
SSWB

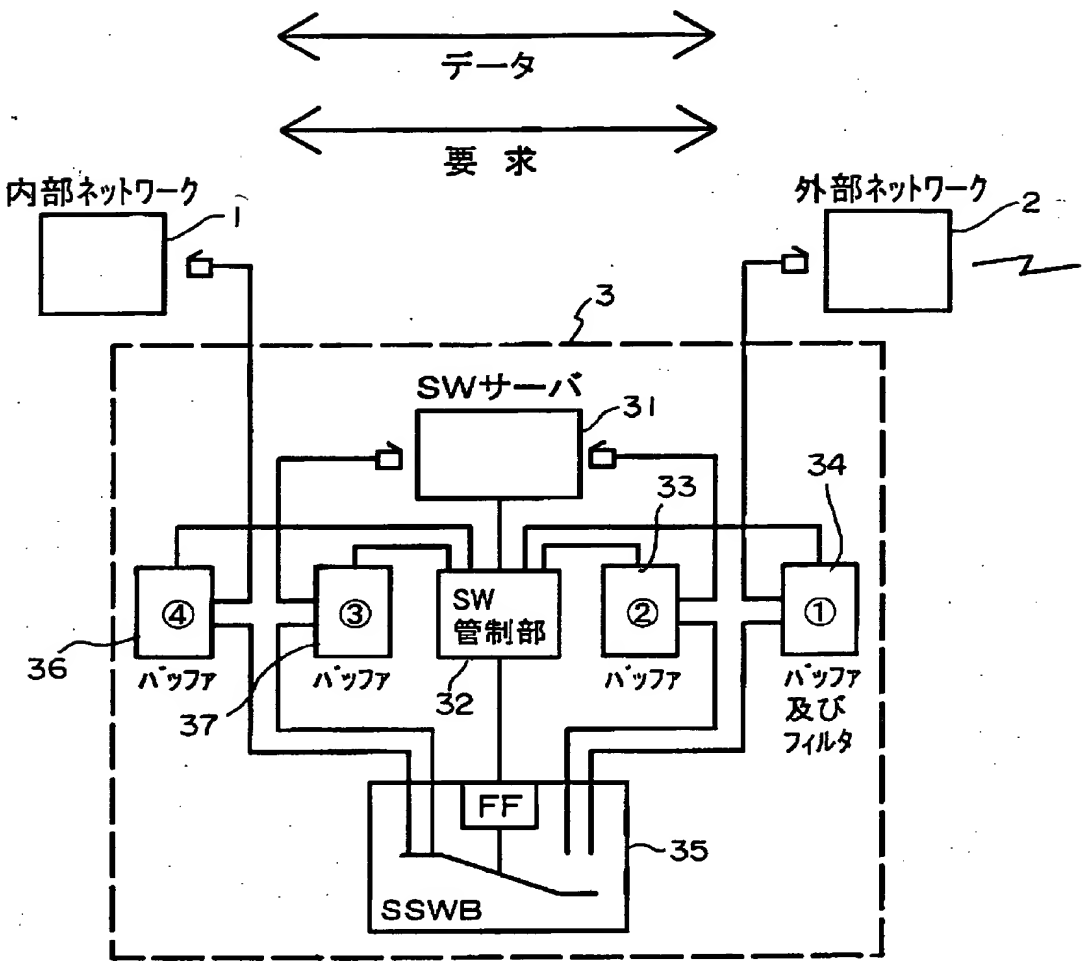
【図２】


データ
要 求
内部ネットワーク
1
外部ネットワーク
2
SWサーバ
31
3
33
32
SW管制部
バッファ
バッファ及び
フィルタ
34
FF
35
SSWB

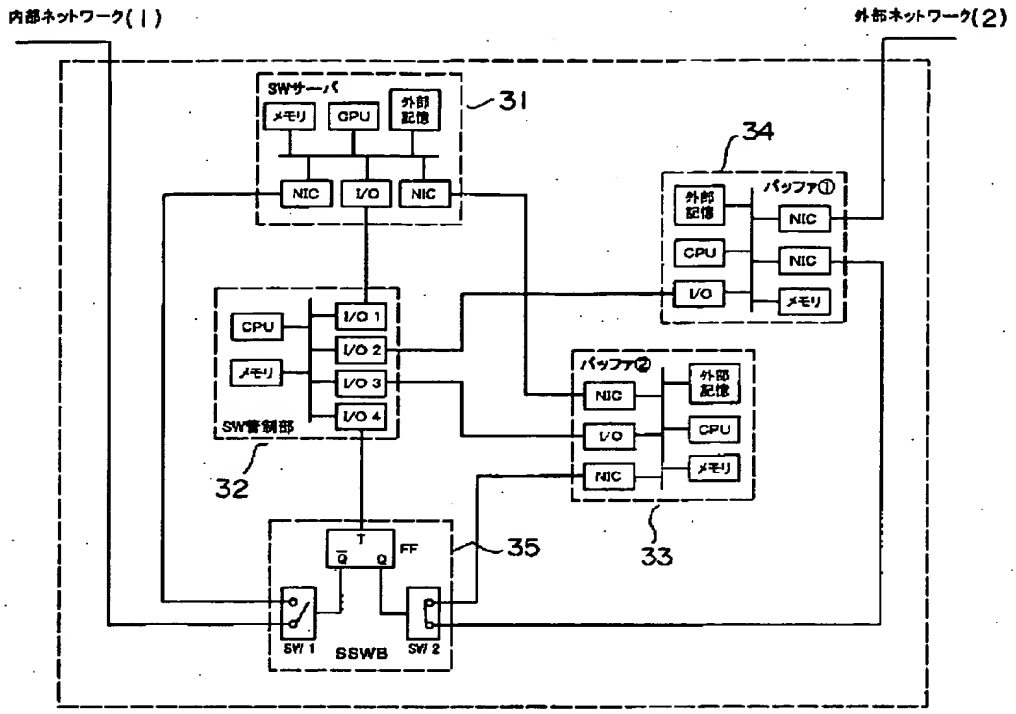
【図３】


データ
要 求
内部ネットワーク
1
外部ネットワーク
2
SWサーバ
31
3
33
34
32
SW管制部
バッファ
バッファ及び
フィルタ
FF
35
SSWB

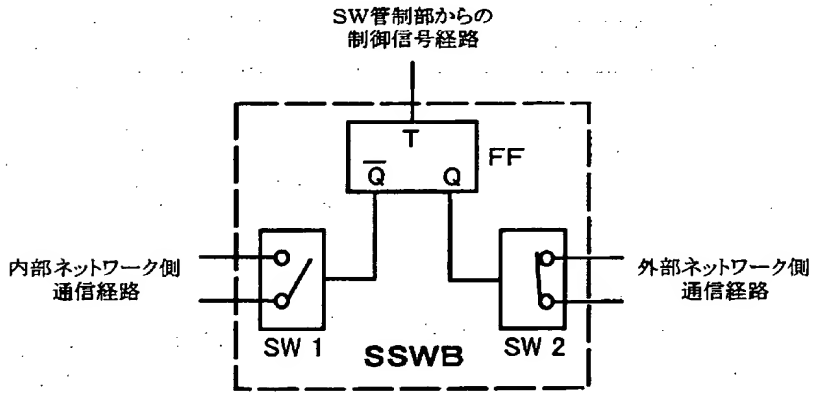
【図４】


データ
要　求
内部ネットワーク
1
外部ネットワーク
2
3
SWサーバ
31
33
34
④
③
SW
管制部
②
①
36
バッファ
バッファ
32
バッファ
バッファ
及び
フィルタ
37
FF
35
SSWB

【図５】



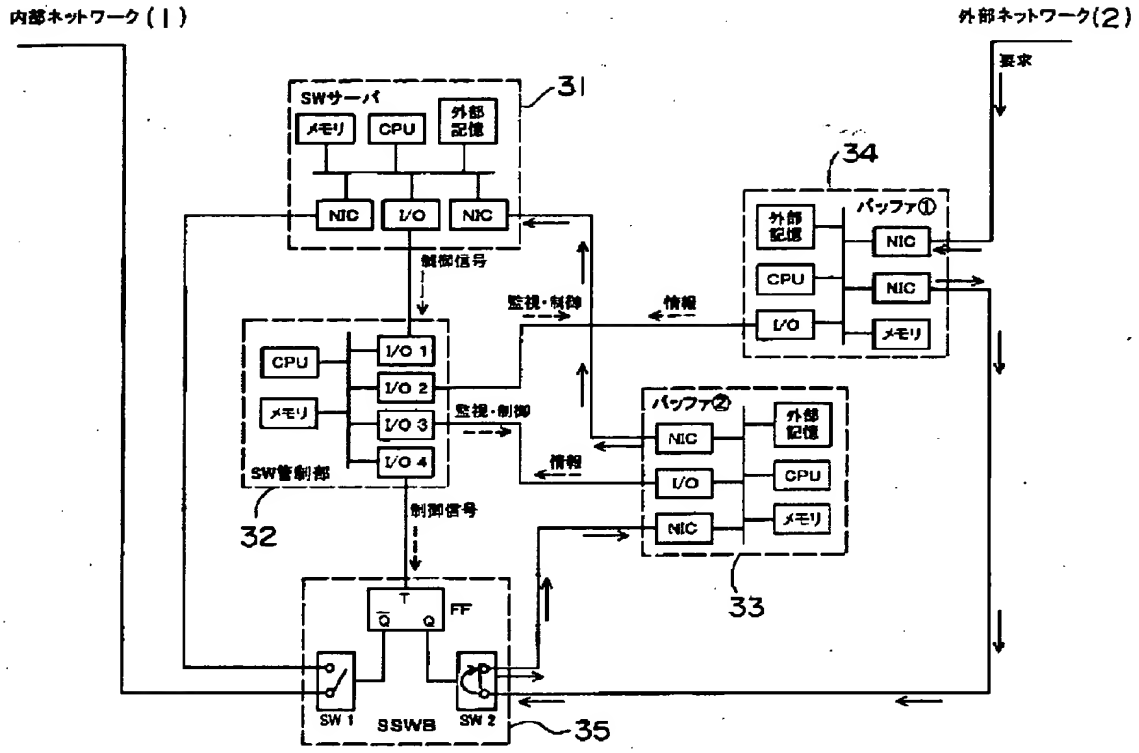
【図６】



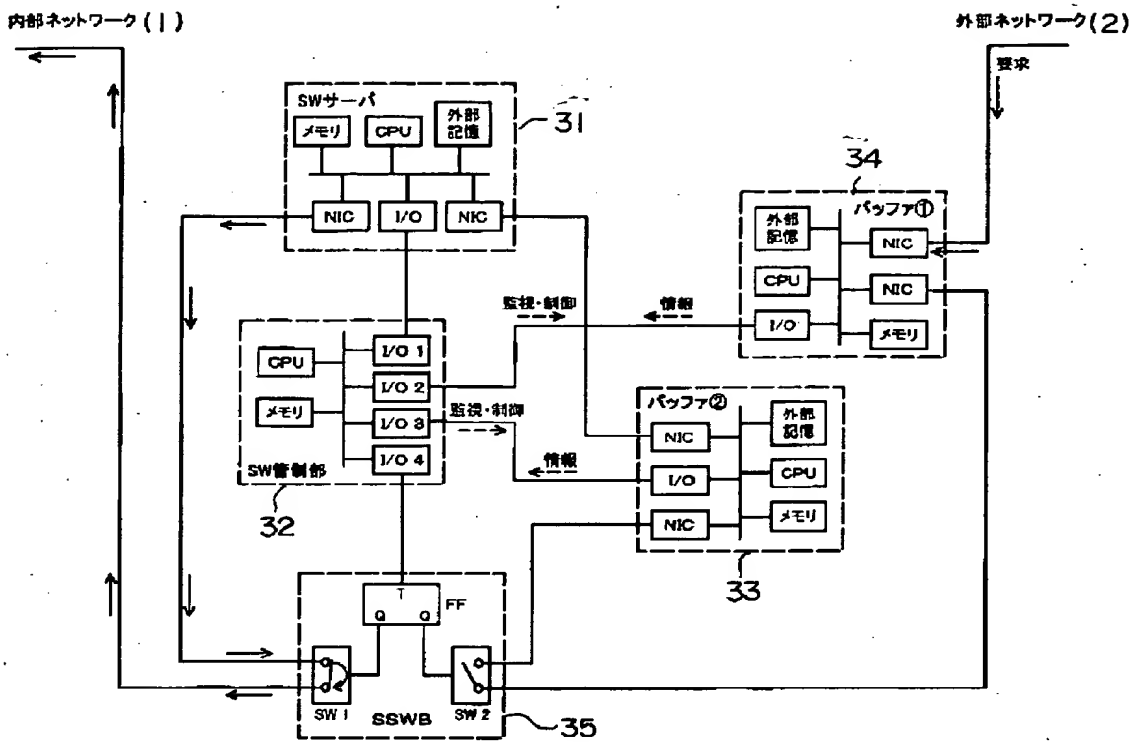
＜ＳＷ１とＳＷ２を制御するカットフリップフロップの真理値表＞

T	Q　　$\overline{Q}$
0	変化しない
1	反転する

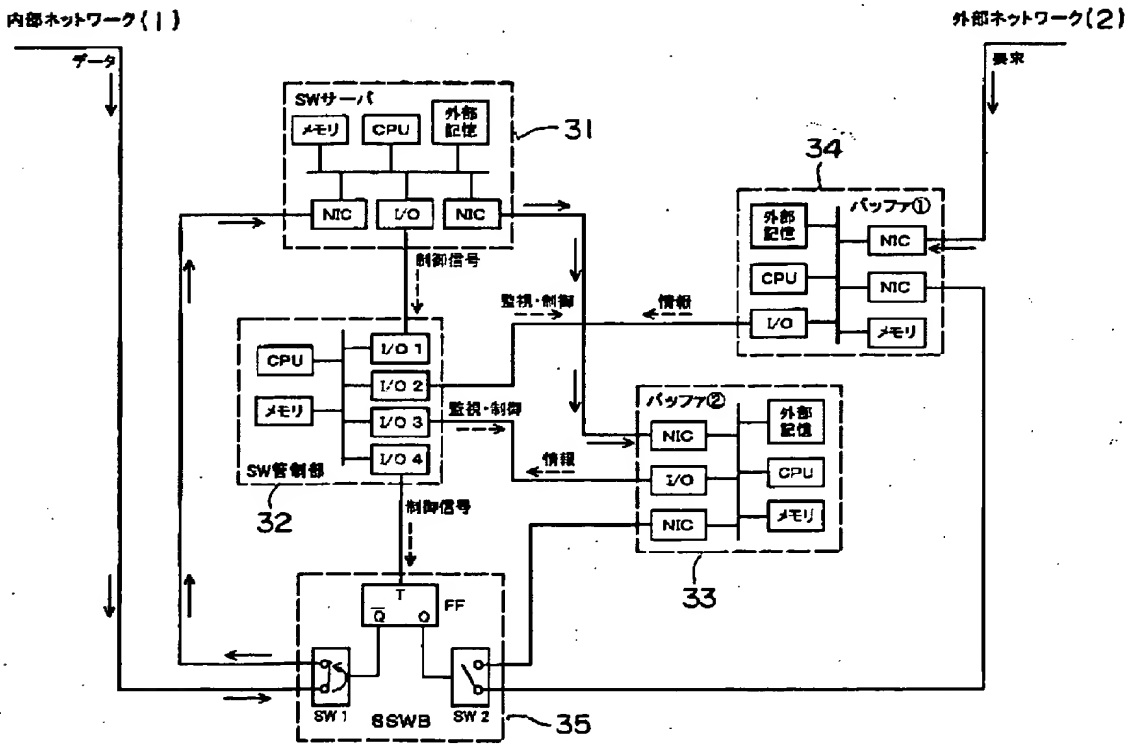
【図７】


内部ネットワーク(1)
外部ネットワーク(2)
要求
SWサーバ
メモリ
CPU
外部記憶
31
NIC
I/O
NIC
制御信号
監視・制御
情報
34
バッファ①
外部記憶
NIC
CPU
NIC
I/O
メモリ
CPU
I/O 1
I/O 2
メモリ
I/O 3
I/O 4
SW管制部
32
監視・制御
情報
制御信号
バッファ②
NIC
外部記憶
I/O
CPU
NIC
メモリ
33
T
Q
FF
SW 1
SSWB
SW 2
35

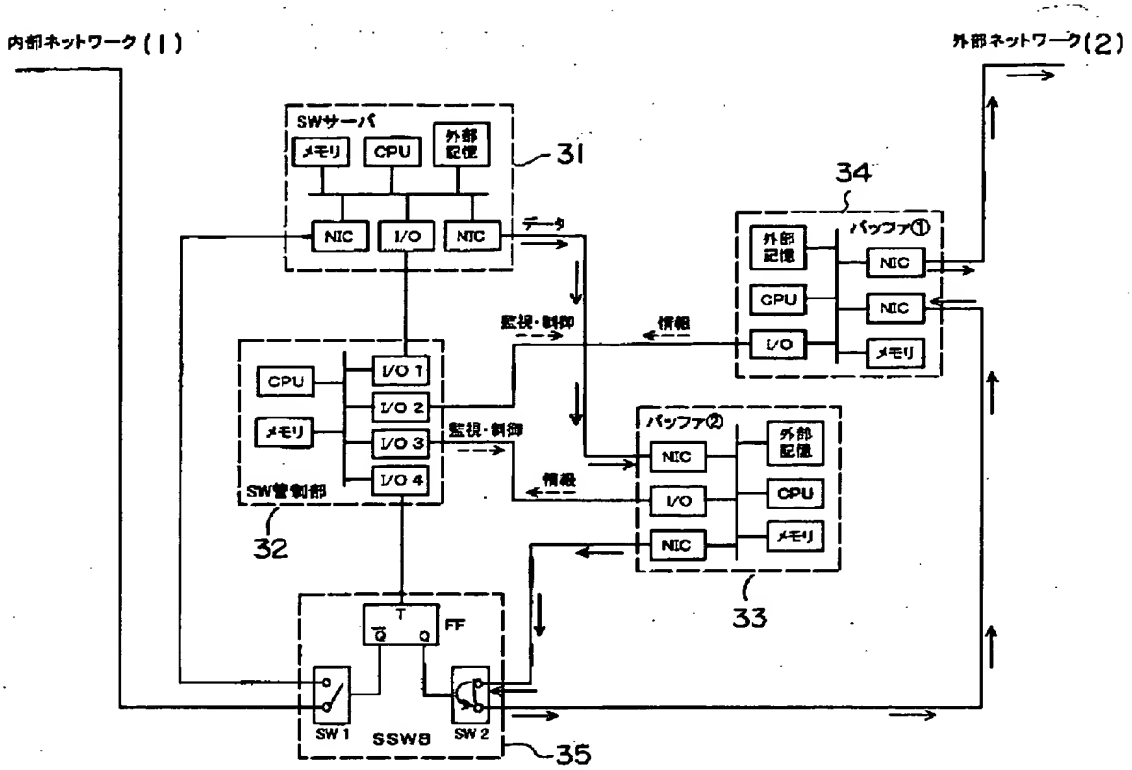
【図８】


内部ネットワーク(1)
外部ネットワーク(2)
要求
SWサーバ
メモリ
CPU
外部記憶
31
NIC
I/O
NIC
34
バッファ①
外部記憶
NIC
CPU
NIC
I/O
メモリ
監視・制御
情報
CPU
メモリ
I/O 1
I/O 2
I/O 3
I/O 4
監視・制御
情報
SW管制部
32
バッファ②
NIC
I/O
NIC
外部記憶
CPU
メモリ
33
T
Q
Q
FF
SW 1
SSWB
SW 2
35

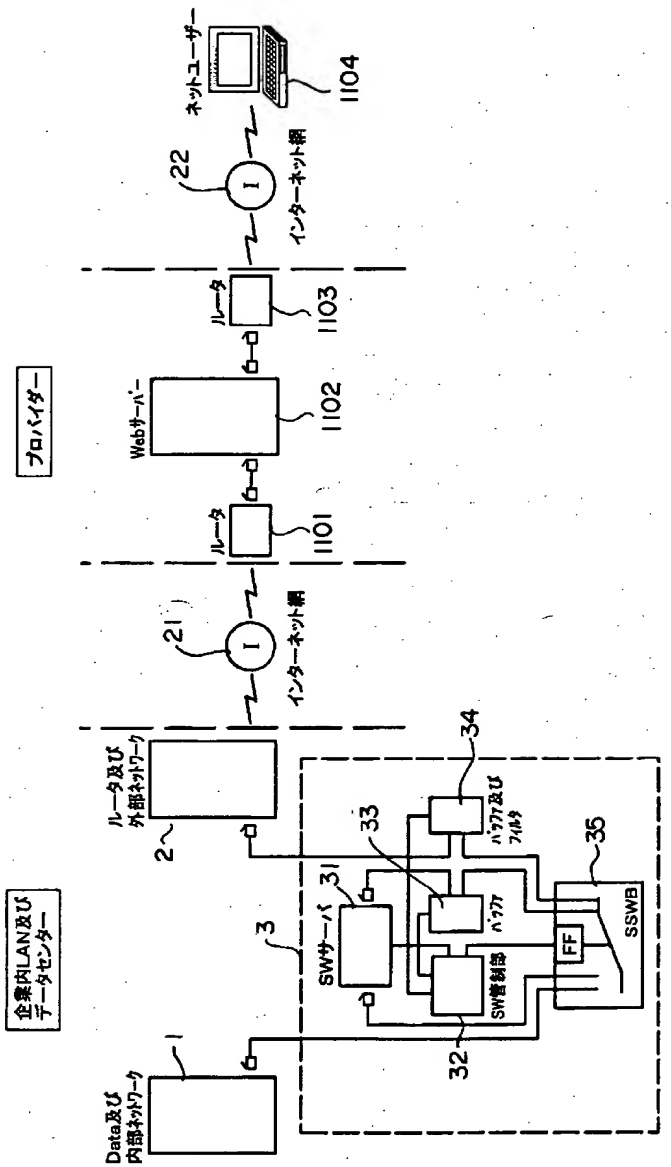
【図９】


内部ネットワーク(1)
外部ネットワーク(2)
データ
要求
SWサーバ
メモリ
CPU
外部記憶
31
NIC
I/O
NIC
34
バッファ①
外部記憶
NIC
CPU
NIC
I/O
メモリ
制御信号
監視・制御
情報
CPU
メモリ
I/O 1
I/O 2
I/O 3
I/O 4
監視・制御
情報
SW管制部
32
制御信号
バッファ②
NIC
I/O
NIC
外部記憶
CPU
メモリ
33
T
Q
Q
FF
SW 1
SSWB
SW 2
35

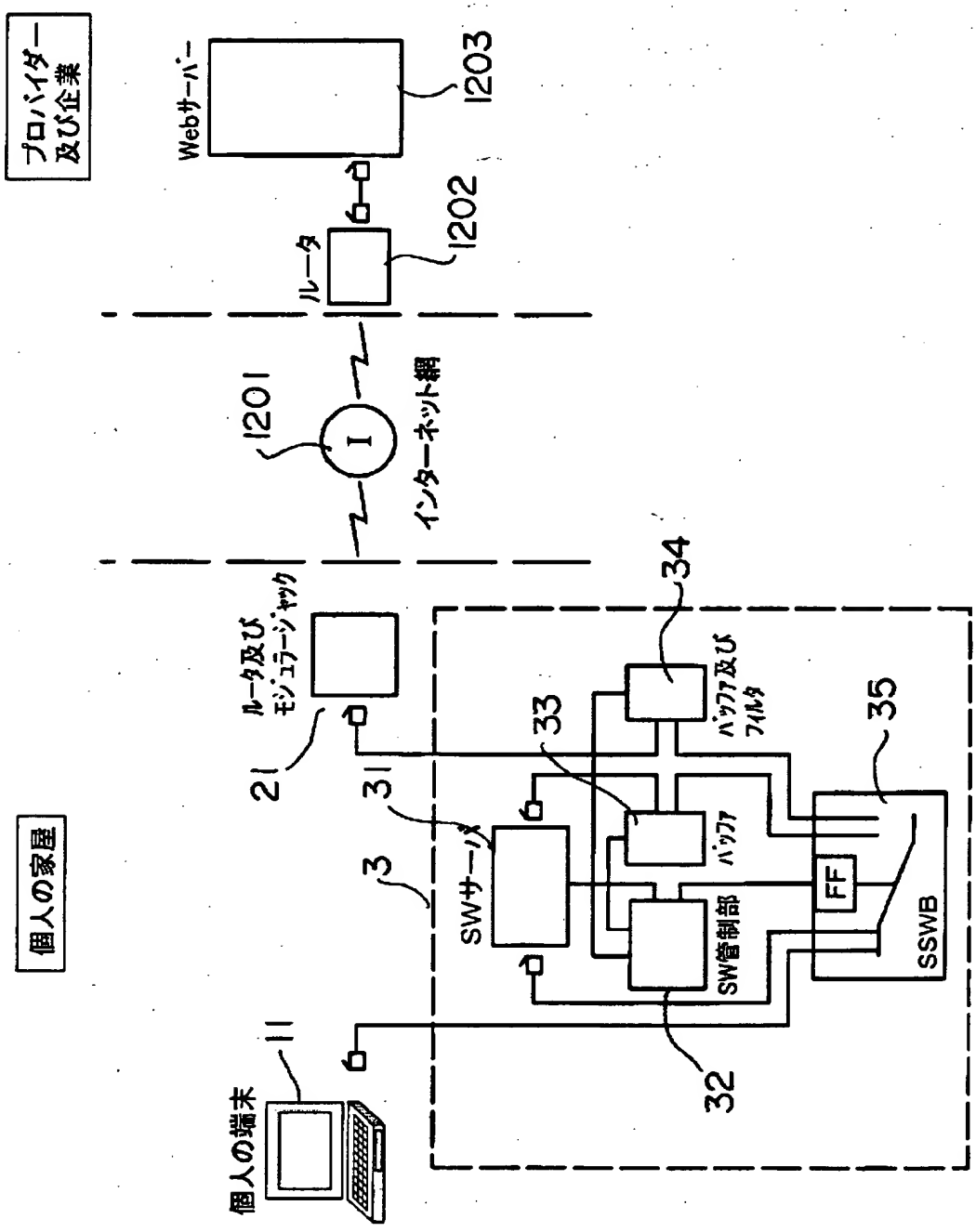
【図１０】


内部ネットワーク(1)
外部ネットワーク(2)
SWサーバ
メモリ
CPU
外部記憶
31
NIC
I/O
NIC
データ
34
バッファ①
外部記憶
NIC
CPU
NIC
I/O
メモリ
監視・制御
情報
CPU
メモリ
I/O 1
I/O 2
I/O 3
I/O 4
監視・制御
情報
SW管制部
32
バッファ②
外部記憶
NIC
I/O
CPU
NIC
メモリ
33
T
Q
FF
SW 1
SSW8
SW 2
35

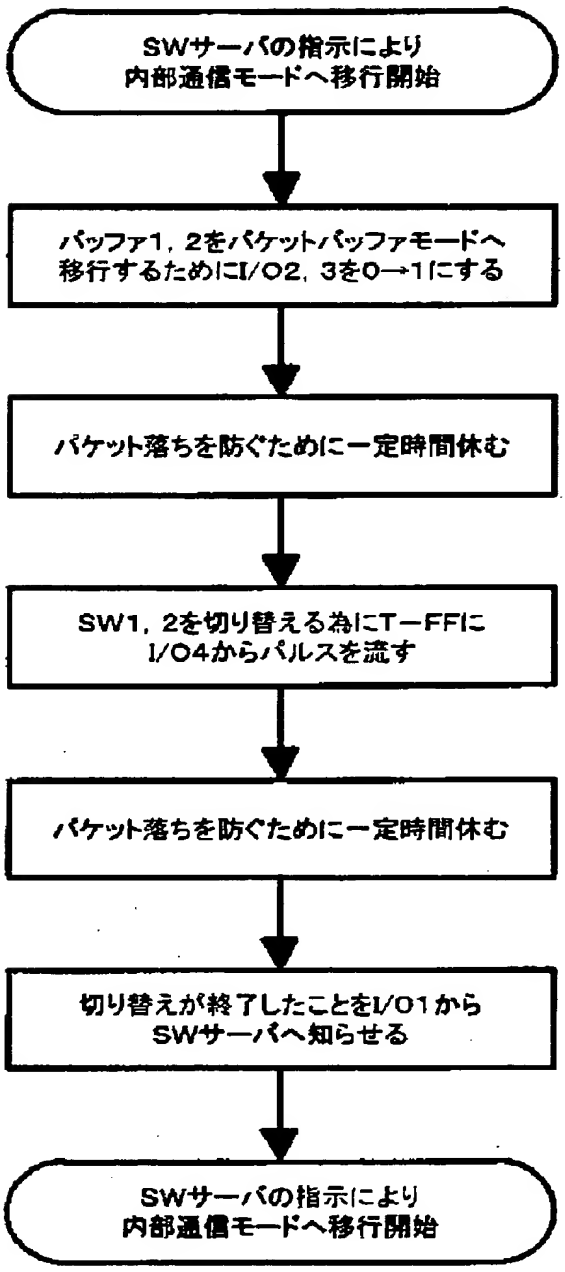
【図１１】


ネットユーザー
1104
22
インターネット網
ルータ
1103
プロバイダー
Webサーバー
1102
ルータ
1101
21
インターネット網
ルータ及び
外部ネットワーク
2
34
ハブ及び
フィルタ
33
35
31
ハブ
SWサーバ
3
SW管制部
FF
SSWB
企業内LAN及び
データセンター
1
32
Data及び
内部ネットワーク

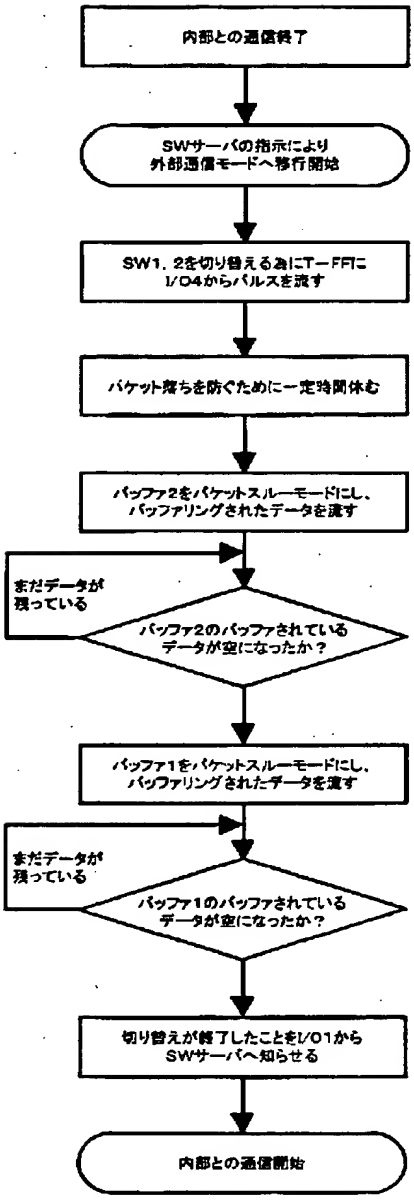
【図１２】


プロバイダー及び企業
Webサーバー
1203
1202
ルータ
1201
インターネット網
個人の家屋
ルータ及びモジュラージャック
21
31
34
バッファ及びフィルタ
33
35
バッファ
3
SWサーバ
FF
SW管制部
SSWB
32
11
個人の端末

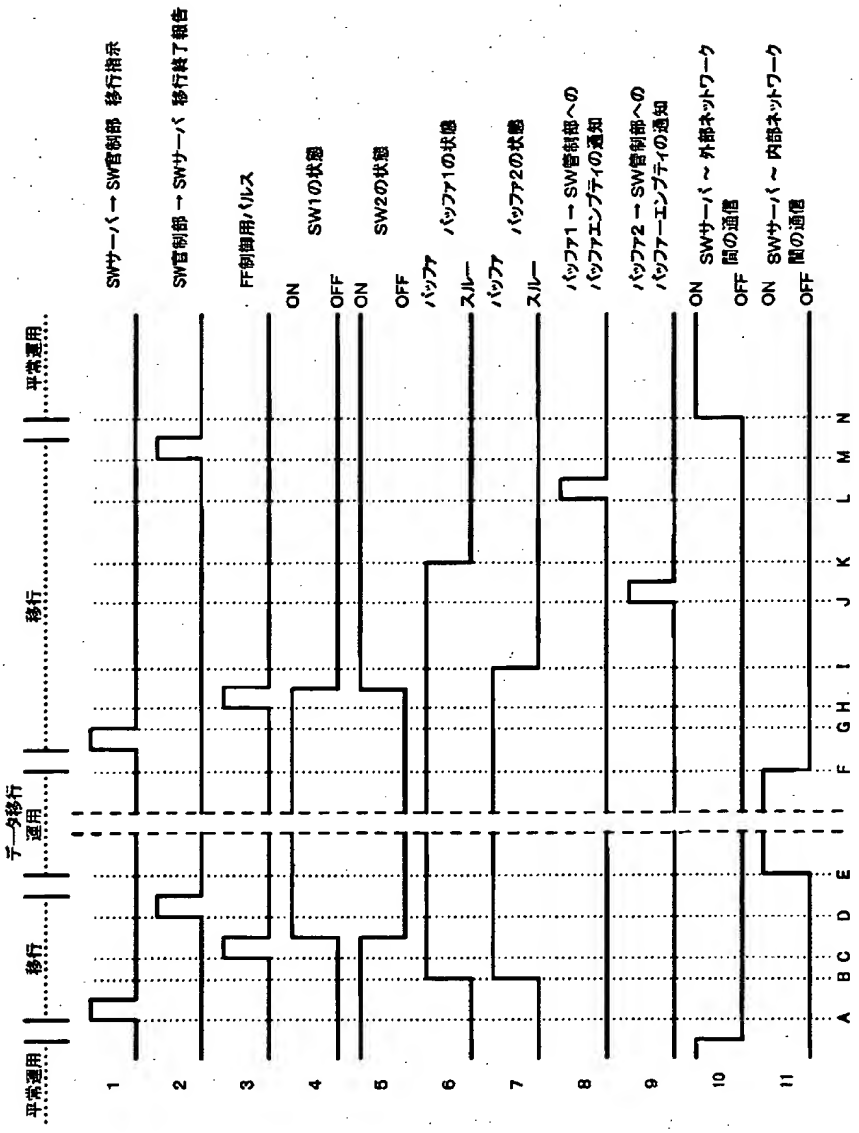
【図１３】


SWサーバの指示により
内部通信モードへ移行開始
バッファ1，2をパケットバッファモードへ
移行するためにI/O2，3を0→1にする
パケット落ちを防ぐために一定時間休む
SW1，2を切り替えるためにT－FFに
I/O4からパルスを流す
パケット落ちを防ぐために一定時間休む
切り替えが終了したことをI/O1から
SWサーバへ知らせる
SWサーバの指示により
内部通信モードへ移行開始

【図１４】


内部との通信終了
SWサーバの指示により
外部通信モードへ移行開始
SW1，2を切り替えるためにT－FFに
I/O4からパルスを流す
パケット落ちを防ぐために一定時間休む
バッファ2をパケットスルーモードにし、
バッファリングされたデータを流す
まだデータが
残っている
バッファ2のバッファされている
データが空になったか？
バッファ1をパケットスルーモードにし、
バッファリングされたデータを流す
まだデータが
残っている
バッファ1のバッファされている
データが空になったか？
切り替えが終了したことをI/O1から
SWサーバへ知らせる
内部との通信開始

【図１５】


平常運用
移行
データ移行
運用
移行
平常運用
SWサーバ→SW管制部 移行指示
SW管制部→SWサーバ 移行終了報告
FF制御用パルス
ON
SW1の状態
OFF
ON
SW2の状態
OFF
バッファ
バッファ1の状態
スルー
バッファ
バッファ2の状態
スルー
バッファ1→SW管制部へのバッファエンプティの通知
バッファ2→SW管制部へのバッファーエンプティの通知
ON
SWサーバ～外部ネットワーク間の通信
OFF
ON
SWサーバ～内部ネットワーク間の通信
OFF
1
2
3
4
5
6
7
8
9
10
11
A
B
C
D
E
F
G
H
I
J
K
L
M
N

【書類名】　　要約書

【要約】

【課題】　外部ネットワークからのアクセスに対し、物理的手段によって内部ネットワーク内への直接的な侵入を防ぎつつ、内部ネットワークと外部ネットワークとの柔軟な連携を可能とする。

【解決手段】　通信路に介在させ、一方側の通信路との接続と、他方の通信路との接続とを排他的に選択する通信路のスイッチ接続制御装置とすることにより、目的別に分散した端末及びシステムに、シーソー式のスイッチング技術を用い不正侵入を防ぐセキュリティシステムを提供する。このようにシーソー式のスイッチング技術により、物理的に外部ネットワークと内部ネットワークとを目的に応じたアクセス要求の制御信号によって切り離すため、不正行為から確実にデータを守ることが可能となる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔５００２８３０８８〕

１．変更年月日　　２０００年　６月１６日
［変更理由］　新規登録
住　所　東京都世田谷区宮坂１丁目３６番１８号
氏　名　株式会社　イオノス